How to Stop DDoS Attacks in Three Stages

Chad Kime October 3, 2023

eSecurity Planet content and product recommendations are editorially independent. We may make money when you click on links to our partners. Learn More.

When under siege from a distributed denial of service (DDoS) attack, systems grind to a halt and often become entirely unresponsive. To stop the attack, defenders must move quickly and navigate three broad response stages:

- **Stage I:** Block the DDoS Attack**:** Take immediate steps to attempt to block the attack, which may require outside assistance or even shutting down the resource. For the steps to stop specific types of attacks see:
  - Stop Internal and External Router, Server, and Website DDoS Attacks
  - Stop External Router or Video Game System DDoS Attacks
- **Stage II:** Determine the Type of DDoS Attack**:** Examine and analyze log files, alerts and other records for clues regarding source and type of DDoS attack — in some cases, this step may also need to be completed to block the attack.
- **Stage III:** Recover from the DDoS Attack**:** Change security architecture, processes, or tools to recover from the current attack and prevent further attacks.

Like all cybersecurity attacks and problems, the fundamentals may be simple, but the execution and the details will be far more complicated. This article explores how to stop DDoS attacks through the following topics:

- Stage I: Block the DDoS Attack
- Stage II: Determine the Type of DDoS Attack
- Stage III: Recover from the DDoS Attack
- The Approximate Nature of the Three Stages
- Prevent Future DDoS Attacks
- Bottom Line: Prepare Now or Suffer Later

Table of Contents

Stage I: Block the DDoS Attack

Stop Specific DDoS Attacks

Stage II: Determine the Type of DDoS Attack

Stage III: Recover from the DDoS Attack

Top Cybersecurity Companies

1 ManageEngine Log360

2 Graylog

3 ManageEngine Desktop Central

4 Safetica

5 Dashlane

See Full List

Get the free newsletter

Subscribe to **Cybersecurity Insider** for top news, trends & analysis

Enter an email

By signing up to receive our newsletter, you agree to our Terms of Use and Privacy Policy.

Sign up

Featured Partners: Cybersecurity Training Software

NINJIO Cybersecurity Awareness Training

ESET® Cybersecurity Awareness Training

Visit Website

Good For

Any Company Size

Core Features

Data Security

Integrations

Azure, Google Workspace, Microsoft 365

Digital Security
Progress. Protected.

Visit Website

Good For

Any Company Size

Core Features

Automated Emails, Dashboard, Gamification, and 2 more

Integrations

LinkedIn

eSecurity Planet may receive a commission from merchants for referrals from this website

Stage I: Block the DDoS Attack

Once under a DDoS attack, resources perform sluggishly and even changes to protect them can be difficult to execute. Although attacks cannot be fully stopped without identifying the attack, identification cannot even be attempted when the systems are so locked up that they cannot be accessed.

The attack must be stopped — even temporarily — to recover internal resources such as the CPU capacity and memory. Organizations that send logs to other resources (segregated storage, SIEM solutions, etc.) may be able to work on Stage I: Block the DDoS Attack and Stage II: Determine the Type of DDoS Attack simultaneously.

Fundamental DDoS Response Tactics

Simple DDoS attacks can often be blocked using skilled internal resources. Yet, keep in mind that even basic DDoS attacks may need to be blocked upstream with the help of the host internet service provider (ISP) or else the blocked DDoS attack traffic can still threaten connection bandwidths and ISP infrastructure.

The number of potential tools, services, and techniques to block DDoS attacks exceed the number of possible types of attack. However, they can generally be categorized into the following categories of tactics:

- Call a DDoS Expert
- DDoS IP Address Filtering
- Migrate to a New IP Address
- Enable Strengthen DDoS Protection Options
- Enable Geo-Blocking
- Shut Down Services
- Implement New Technology

These tactics are listed in a rough order based on the likelihood of success and urgency, but are merely a rule of thumb. For example, even when an organization decides to embrace the first category, Call a DDoS Expert, experts may not be able to act right away and the organization will need to attempt other actions in the meantime.

Similarly, the last category, Implement New Technology, trails the list because it often requires significant research. However, if an organization had already done research that category of action could certainly be taken right away.

Any organization under attack should scan the categories and implement what they believe will offer the greatest chance of success based upon their immediate circumstances. Each category will list pros and cons to help with the decision-making process.

Call a DDoS Expert

Typical internet bot DDoS attacks reach 10–11 GB per second, but record DDoS attacks have reached 50 to 70 million requests per second or 3.47 TB per second. Even large enterprises struggle to block attacks of this scale without professional assistance.

Smaller organizations can call their ISP, which might provide DDoS specialists or enable additional functions to block DDoS attacks. However, ISP options may be limited so some organizations turn to

×

consultants, incident response tools or specialists, managed detection and response (MDR) experts, and other security professionals to stop the attack, improve systems against future DDoS attacks, and recommend other needed DDoS tools and services.

Cloud-based DDoS protection services often provide the most comprehensive option to block DDoS attacks, so organizations often engage or migrate their infrastructure behind the protection of Virtual Private Network (VPN) providers (such as NordVPN, Perimeter 81, and Surfshark) or DDoS Protection service providers (such as Akamai, Cloudflare, and Imperva).

Be sure to whitelist the connection between the service and the system being protected and block other connections so nothing bypasses the DDoS service. However, also keep in mind that even cloud providers cannot prevent DDoS attacks originating within the organization's network.

- **Pros of DDoS response services:**
  - Extremely effective
  - Leverages the scale of cloud resources
  - DDoS specialists use expertise to move faster
  - DDoS experts can block a large range of DDoS attacks in progress and can eliminate paths for future DDoS attacks
  - DDoS professionals keep records of DDoS botnets and can block many before they activate

- **Cons:**
  - If an expert is not already in place, the organization must locate and qualify an expert while under pressure
  - This method will cost more than in-house solutions but may be worth the investment

DDoS IP Address Filtering

A quick look at log files will often reveal a specific set of IP addresses generating most of the DDoS traffic. Blocking these attacking IP addresses can provide temporary relief and allow time to pursue other tactics.

- **Pros of DDoS IP address filtering:**
  - Quick to execute, inexpensive
  - Can buy time for other tactics

- **Cons:**
  - Generally a temporary solution at best
  - Attackers can spoof IP addresses
  - Attackers can easily shift to a different source (often a botnet) leading to a game of whack-a-mole where the defenders are constantly trying to keep up with the attackers.
  - Should also be applied at the ISP level or else the ISP bandwidth will be consumed with traffic that is blocked at the resource (application firewall, internet gateway, local firewall, etc.)

Migrate to a new IP Address

Instead of blocking attackers, defenders can move the resource out of the sights of the DDoS attackers and reroute legitimate traffic to a new IP address.

- **Pros of IP address migration:**
  - Inexpensive, relatively quick
  - Can buy time for other tactics

- **Cons:**
  - Generally a temporary solution because attackers will also find the new location
  - May require significant internal changes for other resources linked to the moved resource

Enable or Strengthen DDoS Protection Options

Organizations can check existing resources (server software, router firmware, etc.) for DDoS protection options that may not yet be activated. For example, enabling DDoS options on routers or adjusting request rate limits.

- **Pros:**
  - Inexpensive and quick

- **Cons:**
  - May not be effective against the current attack
  - Attackers can switch methods easily
  - May not be possible to execute until the DDoS attack subsides

Enable Geo-Blocking

Examination of logs during a DDoS attack may reveal huge traffic spikes from countries that do not usually visit the website. Geo-blocking can block large botnets operating from other countries.

- **Pros:**
  - Inexpensive, quick
  - Can be effective and buy time for other tactics

- **Cons:**
  - A temporary solution since botnets exist within all major countries
  - Blocks legitimate traffic from the blocked regions (and possibly employees traveling to or working from those areas)

Shut Down Services

Although it concedes some victory to the DDoS attackers, sometimes shutting down the system under attack provides the best option. The service or resource can be isolated and hardened against further attack before it is brought back online.

If the specific type of attack is known, a specific service under attack may be shut down instead of an entire resource. For example, in an HTTP GET attack, the DDoS attack might be seeking to download very large PDF files so a defense might be to disable the link to PDF files or disable downloads temporarily without affecting the rest of the website.

- **Pros:**
  - Inexpensive to execute, quick, effective

- **Cons:**
  - Potentially disruptive, especially for full system shutdown
  - Although inexpensive to execute, associated business disruptions may be very costly to the organization

Implement New Technology

This response adds web application firewalls, secure web gateways, DDoS protection appliances or other technologies to protect assets. These tools can inspect and clean traffic before it can reach the resource.

- **Pros:**
  - Can be effective and likely protects against future attacks

- **Cons:**
  - Can be expensive and time-consuming to deploy
  - May consume future resources for upkeep
  - May create delays for deployment because of solution research, shipping, and configuration
  - Does not eliminate issues for ISPs in between the internet and the inspecting tool for external attacks
  - Inspecting tools cannot always scale quickly or handle the largest DDoS attacks

Non-Technical DDoS Responses

Even as the incident response team may be scrambling to cope with the DDoS attack, the organization must still deal with other stakeholders:

- Executives need to be kept up to date
- Employees may need to be notified about the availability of internal resources or alternative methods to accomplish work
- Customers may need to be notified and informed about system status (often done using social media unaffected by the attack)
- If the DDoS attack causes significant damages to the business, cybersecurity insurance companies, regulators (Security and Exchange Commission, etc.), and law enforcement may need to be notified

An organization's management should be prepared to embed non-technical assistance into an incident response team to coordinate, manage, and execute written, verbal, and phone communication with stakeholders. The CFO may even want to embed someone on the team with the authority to authorize expenses or to coordinate the rapid authorization of purchases needed to recover from the DDoS attack.

Also read:

- How to Create an Incident Response Plan
- Disaster Recovery Solutions
- Best Incident Response Tools and Software for 2022

Stop Specific DDoS Attacks

The fundamental DDoS techniques above apply to all attacks, but each type of DDoS attack and affected architecture might only benefit from a few of the tactics. Below, we'll provide focused tactics for specific resources under attack — just keep in mind that specific architectures could require specialized techniques.

In many cases, the fastest way to eliminate the attack will be to call in an expert, especially cloud-based DDoS protection and response services. However, external tools will not work effectively for internal attacks on servers, routers, or internal applications.

Additionally, consultants and new tools may also be expensive. Some organizations will not be able to

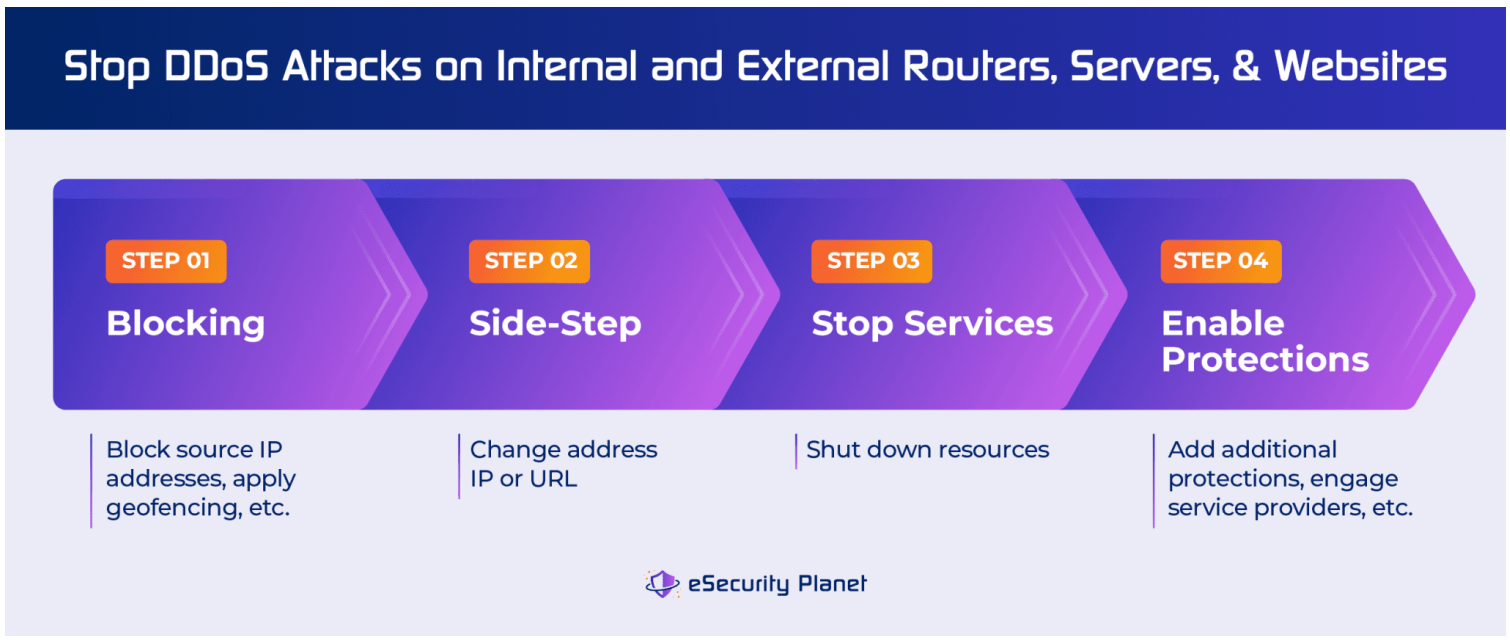
×

authorize immediate use of more expensive resources and other approaches may need to be tried first.

Stop Internal and External Router, Server and Website DDoS Attacks

Assets exposed to the internet for utility, applications and websites often will be targeted by DDoS attackers because they are the easiest to affect. Servers hosting or supporting these resources will often suffer CPU, memory, and bandwidth overload.

These attacks will be very different from internal DDoS attacks on servers and routers, which are based on much older networking protocols and DDoS techniques. Still, once an attack begins, the steps to protect each of these different resources will be quite similar.



Step 1: Block the Initial Attack

It all starts with the evidence buried in the log files. Examine the log files and begin to block the source of the attack by IP address (internal or external), geofencing, or, for internal attacks, even power down compromised local devices generating traffic.

However, there may be circumstances that do not permit shutdown of the DDoS attackers. For example, if an attacker turns the respirator machines of the hospital into a botnet, the hospital cannot simply turn off the respirators without severely affecting patient health.

Additionally, many attackers will be sophisticated enough to switch tactics and sources once they realize the attack has been blocked. Still, while blocking may only be effective temporarily, it will help to buy time for more effective protection to be implemented.

Step 2: Side-step the Attack

If blocking proves ineffective, try changing the server IP address, router IP address, or website URL to move the server out of the path of the DDoS attack. As with blocking the attack, this may only be a temporary reprieve, but it can buy time to implement other tactics that take more time to execute.

Step 3: Stop the Service

If blocking or side-stepping the attack does not work, the organization may need to stop the service under attack (such as a PDF download, shopping cart, internal router, etc.).

Stopping a website, application, or internal network in part or entirely will be so disruptive that this step should not be taken lightly. It should only be pursued if steps 1 and 2 cannot provide enough time to pursue other steps below.

Step 4: Enable Additional Protections

While part of the incident response team attempts to stop the existing attack, other members should be working on enabling other protection against DDoS attacks such as:

- **Call the ISP** to get help or engage external DDoS protection services for websites, applications, and publicly exposed devices under attack (firewalls, servers, routers, etc.)
- **Boost firewall protection** by adding web application firewalls (WAF) or adjust WAF settings to block attacks or rerouting internal traffic through next generation firewalls (NGFW)
- **Boost rate limits** for existing firewalls, servers, and other related resources
- **Engage service providers or add tools**, such as:
  - DDoS protection appliances in front of existing firewall appliances
  - Network security products, network intrusion detection systems (IDS), and intrusion prevention systems (IPS) against internal network attacks
  - WordPress plugins (such as WordFence) to block DDoS traffic
  - Enterprise-level cloud firewalls (such as Google's or FWaaS, Firewall-as-a-Service)
  - DDoS protection service from a vendor such as Cloudflare or Sucuri
  - Incident response or managed IT security service (MSSP) vendor to help locate the malware driving the DDoS attack

However, be aware that additional protections often will affect existing architecture or performance. For

example, load balancers may be bypassed by DDoS tools, or the packet inspection of DDoS protection appliances may introduce lag time for traffic.

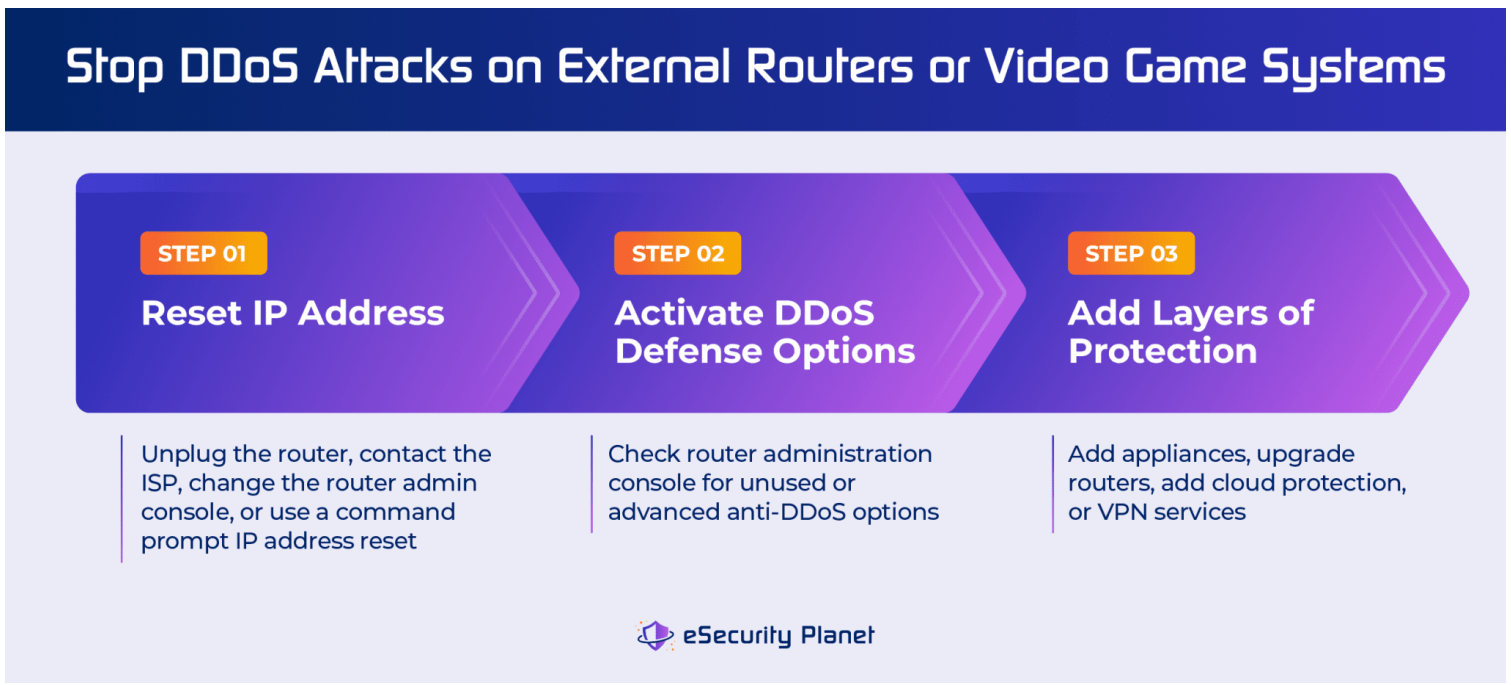
Also keep in mind that a forensic or security investigation will become part of the recovery process, especially for any attack that might trigger cybersecurity insurance claims. The initial infection, access points, malware, and changes to systems introduced by attackers will need to be located and removed to prevent future DDoS attacks or other types of attacks (ransomware, data theft, etc.).

See the Best Digital Forensics Tools & Software for 2022

Stop External Router or Video Game System DDoS Attacks

Attackers need an IP address against which they can launch their DDoS attack. Larger corporations shield their internal IP address with firewalls, and larger video game networks (Steam, official Xbox servers, etc.) hide user IP addresses.

However, small businesses, third-party game servers (such as Minecraft, Team Fortress 2), and video game twitch streamers will often connect their router directly to the internet and attackers can determine the IP address to attack. Often, there is no IT professional regularly supporting the environment so DDoS attacks on these exposed routers and video game machines can result in complete shutdown of internet access.


Stop DDoS Attacks on External Routers or Video Game Systems
STEP 01
Reset IP Address
Unplug the router, contact the ISP, change the router admin console, or use a command prompt IP address reset
STEP 02
Activate DDoS Defense Options
Check router administration console for unused or advanced anti-DDoS options
STEP 03
Add Layers of Protection
Add appliances, upgrade routers, add cloud protection, or VPN services
eSecurity Planet

Step 1: Reset the IP Address

The fastest method to dodge a DDoS attack is to reset the IP address. There are several ways to accomplish this:

- **Fastest method — Unplug:** Unplug the router, game system,and sometimes also the modem. Router IP address reset can take as short as 5 minutes to assign a new IP address or as long as 24 hours, depending upon the ISP.
- **Best method — ISP Contact:** Contact the internet service provider (ISP); some ISPs limit changes in IP address and need to be contacted directly, but ISPs can also implement additional security or offer additional services to block DDoS attacks.
- **Admin console IP Reset:** Log into the router console as an admin via a web browser and change the IP address under Network Settings; check the user manual for instructions for the specific router.
- **Command Prompt IP Address Reset:** Power users can release and renew the IP address using the command line prompts of ipconfig (Windows, MacOS) or ip (Linux) commands; MacOS users can also use advanced system preferences to select TCP/IP and "Renew DHCP Lease."

Of course, this technique renders the internet or network unavailable until the router is restarted, and attackers can still search for the new IP address to attack the router.

Step 2: Activate DDoS Defense Options

Check the manual or the admin console menus on router administration consoles to check for additional DDoS protection options that can be enabled or strengthened. These can be activated quickly, but may affect performance.

Older routers or consumer-grade routers may lack features to protect against modern DDoS attacks and other common network threats. Consider upgrading to more capable devices with more security features or capacity.

Some game consoles have privacy and online safety options available in the menus that can be used to minimize public information. In Xbox, this is called 'private mode' and is available under More Options>Xbox Settings>Privacy and Online Safety.

Step 3: Add Layers of Protection

To block future attacks against routers, consider adding additional layers of protection:

- **Add appliances:** firewalls, Secure Web Gateways (SWG), and DDoS protection appliances can be added between the router and the internet.

- **Upgrade or add professional-grade routers**, next-generation firewalls. For gamers that need to avoid ping increases from packet inspection, look for low-latency devices or devices that can be configured to ignore game-system traffic for inspection.
- **Add cloud-based protection** such as FWaaS or DDoS protection service from a vendor such as Cloudflare or Sucuri.
- **VPN network service** can be added to obscure IP addresses to secure small businesses and streamers; however, it can add ping because of extra network hops. Gamers and streamers can look for VPN services that advertise low-latency connections and secure IP addresses.

The best choice will depend on the budget and technical capabilities of the organization or person as well as how quickly the solution needs to be put into place.

Stage II: Determine the Type of DDoS Attack

Some attacks become obvious because everything grinds to a halt, but often there will be a period in which the resource "acts funny" as it struggles with the early stages of a DDoS attack. In either case, the attack cannot be completely stopped unless it is identified.

In best-case scenarios, security and incident response teams receive sufficient alerts from resources to provide advance warning to cut off the worst of the DDoS attack or to easily analyze the attack. In the worst-case scenarios, log and alerts can only be generated after the resource crashes.

Signs Of DDoS Attack

The first signs of DDoS attack will be delays. Applications will be slow to proceed, websites will be slow to load, servers will be slow to respond to requests, etc.

Users behind an internet connection under attack may find themselves cut off from the internet or unable to use local resources. Network operations centers, firewall monitoring tools, cloud usage tools, and other monitoring solutions may catch spikes in network or internet traffic.

Deep into the attack, resources will simply become unavailable — even to run diagnostic tools or to access log files and other reports. Teams should respond as quickly as possible or ensure resources prioritize sending logs out for analysis.

Examine And Analyze Logs, Alerts, And Records

Log files and other records will keep track of the application performance, network bandwidth, CPU usage, memory usage, and other key factors related to the DDoS attack. Often, the DDoS attack will be a surge in unusual behavior such as sudden increases in web traffic, requests for specific documents, etc.

> **TIP:** Document everything. These records from the DDoS attack will be valuable for calculating damages for cybersecurity insurance, for forensic analysis regarding the attacker, and for the post-mortem analysis of how to prevent similar attacks in the future.

Ideally, the first indicators of trouble will come from alerts set up on monitoring software checking for bandwidth, memory, or CPU issues. Alerts can help a response team jump into action and prevent the DDoS attack before it takes down resources.

Without alerts, an organization may have to rely upon customer or internal complaints which may be delayed because they may also travel through the congested resource (application, server, etc.) crippled by the DDoS attack.

Attack Characterization

Attack characterization helps to discriminate attack traffic from legitimate traffic and to profile the attack itself. Low-level attacks using protocols to disable infrastructure will require a different style of response than an application-level attack attempting to target a specific function in an application.

With so many different types of possible DDoS attacks, it can be difficult to determine exactly which one may be deployed. However, the response team will use their analysis of the logs to provide clues regarding the attack and potential defenses.

Forensic investigation may be required for internal network DDoS attacks to determine how the attack entered the network, infected systems, and launched the DDoS attacks. Specialized forensic investigators will often be required to gather evidence and ensure more sophisticated attackers have been removed from the network.

Attack Traceback

DDoS attack traceback seeks to locate attack sources regardless of the spoofed source IP addresses during or after the attack. During the attack, if the attacks originate from a small number of IP addresses,

the attack can be blocked through IP Blocking; however, this will not be typical for a modern DDoS attack.

Stage III: Recover from the DDoS Attack

Organizations that can quickly eliminate a DDoS attack may suffer no more than inconvenience. Organizations that are not so fortunate will need to assess the damage, make any needed adjustments required from the DDoS remediation, determine what immediate steps to take for preventing recurrence of that DDoS attack, and consider other preventative measures.

DDoS Attack Damage

Damage from DDoS attacks will vary from organization to organization and will depend upon the resources affected. In customer surveys:

- Imperva estimates the average DDoS to cost organizations $40,000 per hour
- Kaspersky's survey shows that the average DDoS attack against an SMB costs $120,000 to resolve, and for enterprises that average increases to $2 million per event.
- Corero's survey estimates direct cost to organizations of $50,000 per DDoS event but does not capture business losses, loss of reputation or other costs.

After a significant DDoS attack, organizations will need to document their costs and damages for two key purposes:

- The damages may be covered by cybersecurity insurance
- The damages create an estimate that can be used to budget for tools and services to prevent future DDoS attacks.

DDoS Remediation Adjustments

In the mad dash to block the DDoS attack, the organization may make architecture or software changes that break connections or cause other issues. Part of the recovery process requires examining the infrastructure to detect and fix those broken components or links.

For example, when moving a website behind a DDoS filtering service provider such as Cloudflare typically only moves the main domain. Sub-domains may not migrate automatically and will require manual adjustments.

Similarly, integration with other third-party tools may require adjustments. For example, a publishing website could discover that their Drupal web content management system no longer correctly connects to the published content protected by the DDoS provider and that a separate Edit sub-domain may be required.

For DDoS attacks launched within the network, individual computer systems may need to be sanitized to remove malware or an attacker's ability to access the device for future attacks. Sometimes this may also trigger data and system recovery needs.

DDoS Attack Lessons Learned

Generate a lessons-learned report that explains the DDoS attack and determines mitigations to protect against similar attacks. Mitigation should be enacted immediately, but if that is not practical, the mitigation should be planned and proposed for budgeting.

The costs to remediate the DDoS attack and any business losses from the downtime will provide a rough target for comparison with the mitigation budget.

If the attack was significant in size or impact, report the incident to law enforcement or industry organizations such as CERT. Reporting attacks can help law enforcement build profiles of major attackers and possibly take steps such as:

- Disrupt command and control infrastructure for Emotet Botnet
- Seize domains from the ZLoader botnet gang
- Coordinated law enforcement takedown of RSOCKS botnet

The Approximate Nature of the Three Stages

Although numbered, incident response teams will often find that some of these stages may need to be executed simultaneously. Additionally, as attackers observe the defender's actions, attackers will often change tactics and require the defending team to iterate between these stages and the steps within them.

Of course, the specifics of each stage will also be highly customized and will depend upon many factors, starting with the type of DDoS attack, the resource under attack (router, website, app, server, etc.), and the DDoS protections or mitigations already in place. Additionally, the IT architecture, the resources of the defender, and the dedication of the attacker will also play significant roles in how the stages and techniques must be navigated.

×

Fortunately, Internet Service Providers (ISPs) and specialist vendors can provide professional **DDoS Protection Services** for immediate assistance for those in need. However, even these security professionals will perform the same tasks we cover here, only with more experience and potentially more sophisticated tools.

The OSI Model and DDoS Attacks

All communication between devices on a network send as network packets containing a packet header, payload, and trailer. As each computer or firewall receives the packet, the device will check for the contents and handle the packet according to the instructions in the header.

DDoS attacks abuse these packets and attempt to exploit potential handling weaknesses to overload systems. The different layers of the OSI model can be used to in DDoS attack classification of the many types of DDoS Attacks:

#	Layer Name	Traffic Type	DDoS Attack Types
1	Physical	Bits crossing hardware	No attacks at this level
2	Datalinks	Frames for addressing	No attacks at this level
3	Network	Packets for delivery	UDP reflection attacks, Ping of Death, etc.
4	Transport	Segments for reliable communication	ACK floods, SYN floods, etc.
5	Session	Data for Interhost communication	Telnet exploits (should be obsolete)
6	Presentation	Data representation and encryption	SSL abuse
7	Application	Data for application use	DNS query floods, HTTP floods

However, this classification tends to be mostly academic. When under attack, knowing which layer an attack might be exploiting does very little to help block or stop the attack. At their essence, all attacks generally fall into two categories:

- **Infrastructure Layer Attacks (Layers 3, 4)**
  - These DDoS attacks affect firewalls, servers, and routers with volumetric or malformed packet attacks
  - ISPs and hosting partners can typically help with these attacks if they are external
  - Internal attacks (on routers, etc.) require firewall or IPS filtering
- **Application Layer attacks (layers 6, 7)**
  - These DDoS attacks are against websites and applications and they way they handle information requests
  - Potentially stopped by web application firewalls (WAF)
  - May require modified website or application design such as adding captcha or other means to block automated requests

Prevent Future DDoS Attacks

After executing the three critical stages to stop a DDoS attack, an organization will find themselves in a better position. However, recovery alone cannot prevent future DDoS attacks because they only address the last attacks. The best way to stop a distributed denial of service (DDoS) attack will always be to be prepared for one in advance.

IT and security teams can deploy many options in preparation for a DDoS attack that will help to control and manage the future impact when a DDoS attack occurs. Vendors, tools, and planning can combine to create a robust and layered approach to limit risks associated with DDoS and lessen the damage from successful DDoS attacks.

An organization also should consider the possible motivations of the attackers. Some DDoS attacks may be used as a distraction or cover-up for other attacks such as espionage, ransomware, or business email compromise. Any DDoS playbook should also include activating a more general incident response to check for other attacks and compromises.

The five key steps to prevent against DDoS attacks include:

1. Harden against attacks
2. Deploy Anti-DDoS Architecture
3. Deploy Anti-DDoS Tools
4. Design a DDoS Response Playbook
5. Deploy DDoS Monitoring

Further reading: How to Prevent DDoS Attacks: 5 Steps for DDoS Prevention

×

Anti-DDoS Vendors

When selecting vendors for anti-DDoS tools or services, it is important to work with DDoS specialists. However, these vendors, like any other IT measures, should fit into the overall IT and security strategies that provide fundamental defense against DDoS attacks on websites (web application firewalls, etc.), applications (application security, etc.), or networks (firewalls, etc.).

While a significant threat, anti-DDoS measures should not be so optimized that they compromise other priorities for operations and security. Here are a few web application firewall options that will help mitigate DDoS attacks.

AppTrana

Visit website

AppTrana is a fully managed Web application firewall, that includes Web application scanning for getting visibility of application-layer vulnerabilities; instant and managed Risk-based protection with its WAF, Managed DDOS and Bot Mitigation service, and Web site acceleration with a bundled CDN or can integrate with existing CDN. All of this backed with a 24×7 Managed Security Expert service to provide custom rules and policy updates with zero false positive guarantee and promise.

Learn more about AppTrana

Cloudflare

Visit website

Cloudflare is a web infrastructure and cybersecurity company founded in 2009 and located in San Francisco, California. Specializing in content delivery network (CDN) services from protecting organizations at the network edge to mitigating DDoS attacks, the Cloudflare WAF protects almost 25 million websites. With a network of that size, Cloudflare offers the latest threat intelligence at scale.

Learn more about Cloudflare

F5

Visit website

Seattle-based F5 traces its roots to the mid-1990s with the release of the BIG-IP load balancer. As the company added appliances, software, and solutions-oriented application layer security, the development of the F5 Advanced WAF became inevitable. From behavioral analytics and machine learning to in-browser data encryption and an anti-bot mobile SDK, F5 offers industry-leading features. F5 is consistently a top alternative for users adopting other WAF solutions.

Learn more about F5

Pros and Cons of DDoS Infrastructure Types

When considering tools for protection, the solutions often break down into three classifications: Do-it-yourself (DIY), on-premises appliances, and off-premises tools. Each style has inherent pros and cons.

- **DIY tools** can be created from Open Source Tools
  - **Pros:** lower cost, compatible with fully controlled and third-party hosted assets
  - **Cons:** deployed reactively, requires expertise to integrate and use, limited filtering capabilities, not scalable
  - **Most suited for** organizations with constrained budgets and less valuable resources to protect
- **On-premises appliances** can be purchased and installed locally
  - **Pros:** good filtering capabilities, less expertise required to integrate and use
  - **Cons:** more expensive, deployed reactively, limited scalability, only compatible with owned and dedicated infrastructure
  - **Most suited for** organizations with requirements for full infrastructure control and with less targeted infrastructure that will not suffer from the limited scalability of appliances
- **Off-premises ddos protection** are cloud-hosted tools, often SaaS
  - **Pros:** always on or automated, unlimited scalability, easy to use and integrate, compatible with fully controlled and third-party hosted assets
  - **Cons:** more expensive
  - **Most suited for** organizations with high value assets exposed to DDoS attacks that will benefit from the speed and scalability of cloud protection

Ultimately, the tradeoffs revolve around cost, speed, and control. DIY tools will always cost the least and offer full control, but will not respond quickly or scale easily to handle large attacks. Scaling represents capacity, but also directly affects speed since a device that is over its capacity lengthens the time for recovery.

On-premises appliances can enable more speed and full control, but will cost more and have limited scale. Cloud-hosted tools will always react faster and can deploy nearly unlimited scale, but will cost more and also lie outside of the direct control of the organization.

Bottom Line: Prepare Now or Suffer Later

With the increasing sophistication and capabilities of attackers, defenders must be on alert. Not only will stopping DDoS attacks become increasingly difficult, but attackers will continue to increase the speed at which they exploit windows of opportunity. Organizations should prepare now for future DDoS attacks and take advantage of the capable tools and services available to help them.

See the Best Bot Protection Solutions

Previous article

Weekly Vulnerability Recap – October 2, 2023 – WS_FTP, Exim, Cisco and Other Exploited Vulnerabilities

Next article

Kali Linux Penetration Testing Tutorial: Step-By-Step Process

Chad Kime

eSecurity Planet lead writer Chad Kime covers a variety of security, compliance, and risk topics. Before joining the site, Chad studied electrical engineering at UCLA, earned an MBA from USC, managed 200+ ediscovery cases, and helped market a number of IT and cybersecurity products, then transitioned into technical writing policies and penetration test reports for MSPs and MSSPs. In his free time, Chad enjoys walks on the beach with his wife, annoying his children, and trying to carve out time for movies, books, video games, and bike rides.

Subscribe to Cybersecurity Insider

Strengthen your organization's IT security defenses by keeping abreast of the latest cybersecurity news, solutions, and best practices.

Enter an email

By registering, you agree to the Terms of Use and acknowledge the data practices outlined in the Privacy Policy. You may unsubscribe from these newsletters at any time.

Subscribe

Related Articles

5 Best Cybersecurity Certifications to Get in 2025

NETWORKS October 31, 2024

7 Best Attack Surface Management Software for 2025

NETWORKS October 25, 2024

How to Set Up a VLAN in 12 Steps: Creation & Configuration

NETWORKS October 24, 2024

eSecurity Planet

eSecurity Planet is a leading resource for IT professionals at large enterprises who are actively

×

researching cybersecurity vendors and latest trends. eSecurity Planet focuses on providing instruction for how to approach common security challenges, as well as informational deep-dives about advanced cybersecurity topics.

© 2024 TechnologyAdvice. All Rights Reserved.